aiim eBook

Intelligent Information Management

Information Privacy and Security

GDPR is Just the Tip of the Iceberg

by John Mancini and Andrew Pery

In Partnership with

filefacets

aiim

About AIIM

AIIM has been an advocate and supporter of information professionals for nearly 70 years. The association mission is to ensure that information professionals understand the current and future challenges of managing information assets in an era of social, mobile, cloud and big data.

AIIM builds on a strong heritage of research and member service. Today, AIIM is a global, non-profit organization that provides independent research, education and certification programs to information professionals. AIIM represents the entire information management community: practitioners, technology suppliers, integrators and consultants.

AIIM runs training programs — including programs on privacy and governance — which can be found at http://www.aiim.org/Training

© 2017

AIIM
1100 Wayne Avenue, Suite 1100
Silver Spring, MD 20910
(+1) 301 587-8202
www.aiim.org

AIIM Europe
Office 1, Broomhall Business Centre,
Broomhall Lane, Worcester, WR5 2NT, UK
+44 (0)1905 727600
www.aiim.org

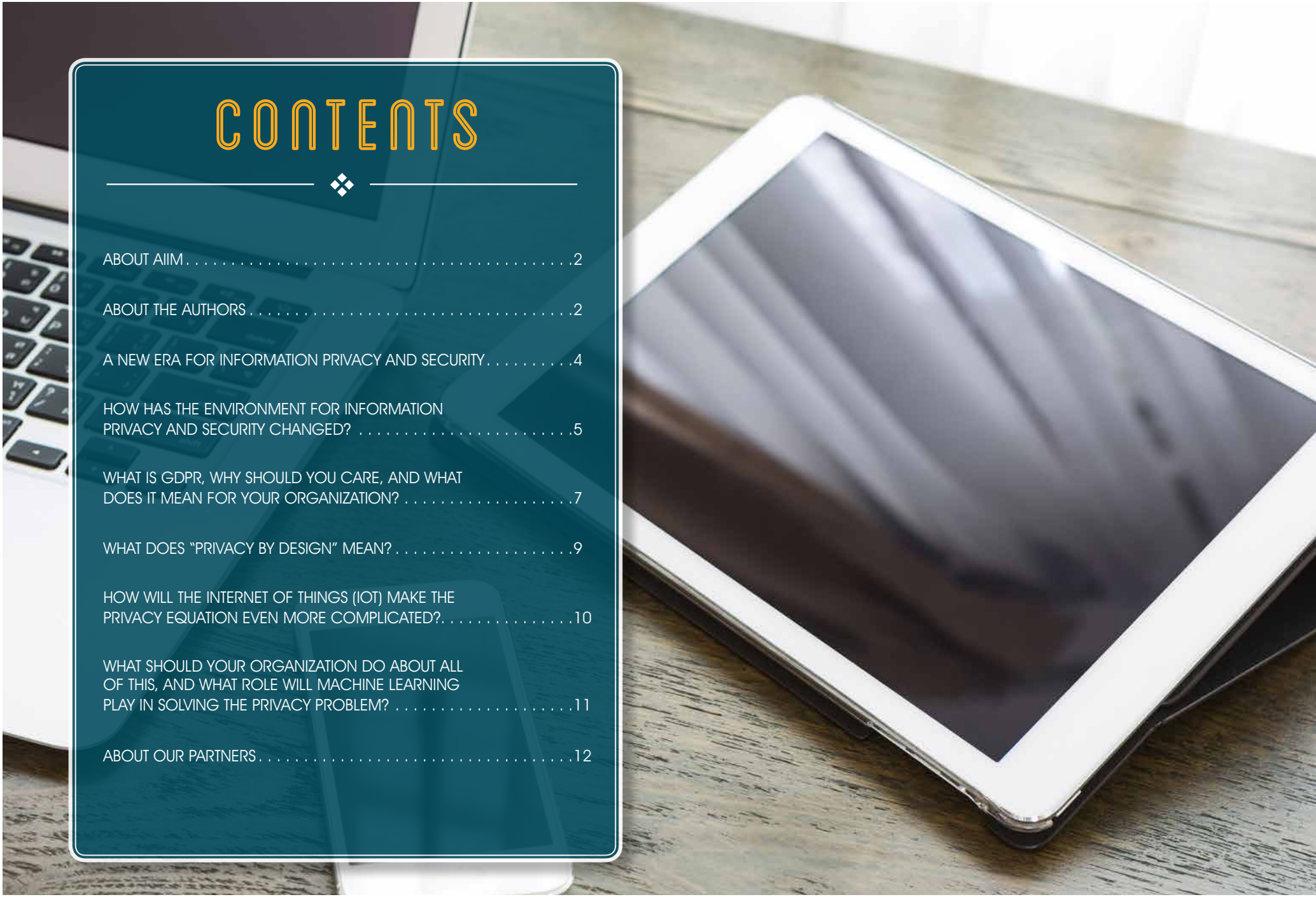
About the Authors

John Mancini
Chief Evangelist
AIIM

John Mancini is Chief Evangelist for AIIM. As a frequent keynote speaker, John offers his expertise on Digital Transformation and the struggle to overcome Information Chaos. He blogs under the title "Digital Landfill" and has more than 11,000 Twitter and 5,000 LinkedIn followers. John can be found on Twitter, LinkedIn and Facebook as **jmancini77**

Andrew Pery
Marketing Executive

Andrew Pery is a marketing executive with over 25 years of experience in the high technology sector focused on content management and business process automation Andrew holds a Masters of Law degree with Distinction from Northwestern University is a Certified Information Privacy Professional (CIPP/C) and a Certified Information Professional (CIP/AIIM).



CONTENTS

ABOUT AIIM 2

ABOUT THE AUTHORS 2

A NEW ERA FOR INFORMATION PRIVACY AND SECURITY 4

HOW HAS THE ENVIRONMENT FOR INFORMATION PRIVACY AND SECURITY CHANGED? 5

WHAT IS GDPR, WHY SHOULD YOU CARE, AND WHAT DOES IT MEAN FOR YOUR ORGANIZATION? 7

WHAT DOES "PRIVACY BY DESIGN" MEAN? 9

HOW WILL THE INTERNET OF THINGS (IOT) MAKE THE PRIVACY EQUATION EVEN MORE COMPLICATED? 10

WHAT SHOULD YOUR ORGANIZATION DO ABOUT ALL OF THIS, AND WHAT ROLE WILL MACHINE LEARNING PLAY IN SOLVING THE PRIVACY PROBLEM? 11

ABOUT OUR PARTNERS 12

Information Privacy and Security:

GDPR IS JUST THE TIP OF THE ICEBERG

By John Mancini and Andrew Pery

The case for more rigorous cybersecurity and the protection of personally identifiable information is compelling Consider the following:

- *The Identity Theft Resource Center found that data breaches have increased 40% from 2015 to 2016, reaching an all-time high of 1,093 in the U.S. alone.*
- *The average cost per breach in 2016 is pegged at $4 million, up 29% from the year prior.*
- *The 2016 Telstra Cybersecurity Report found that nearly 60% of organizations surveyed lack sufficient cyber security and privacy staff to handle increasing legal compliance demands and new information security best practices.*
- *In September 2017, credit bureau Equifax — the very place where many customers go to determine whether their identity has been compromised — revealed that private information for 145.5 million customers had been compromised. At a recent Congressional hearing to determine the cause of the breach, the former Equifax CEO testified that it was due to a combination of human and technical failures. Equifax was notified earlier this year by the Department of Homeland Security to fix a potential vulnerability in their disputes portal. However the patch was not applied in a timely fashion due to internal communications failures within Equifax. This led to an initial breach on May 13, a full three months before the company notified consumers on August 15.*

These troubling trends are prompting regulators to bolster data security and privacy legislation to impose stricter obligations on businesses and data controllers. Europe's new General Data Protection Regulation (GDPR) is the most immediately visible evidence of what will soon be a tidal wave of national and industry information privacy and security regulations.

Organizations cannot hope to meet this coming wave of regulation by approaching information privacy and security as an afterthought or by applying outdated and manual approaches to a set of problems that simply must be automated.

In this e-book, we focus on five key questions that should be on every C-level executive's list of priorities:

- *How has the environment for information privacy and security changed?*
- *What is GDPR, why should you care, and what does it mean for your organization?*
- *What does "Privacy by Design" Mean?*
- *How will the Internet of Things make the privacy equation even more complicated?*
- *What should your organization do about all of this, and what role will machine learning play in solving the problem?*

1 How has the environment for information privacy and security changed?

In an 1890 Harvard Law Review article — yes, 1890 — the authors coined the phrase "the right to be left alone" as a key tenet of privacy law

This definition of privacy was conceived for the analog world. Today, consumers are subject to unprecedented incursions to their privacy. The juxtaposition of big data, cloud computing, predictive analytics and the Internet of Things enables organizations to collect and process vast amounts of information. Taken together, these create a digital fingerprint of behaviors that may expose personally identifiable information. There seems to be a sense of capitulation that in this digital age, privacy rights are destined to erode.

The amount of personal data stored by companies and governments has ballooned, and the value of that data has multiplied as more and more personal business is transacted on the internet. Identity theft has become far more prevalent. In addition to the disruption to businesses and the impact on customer loyalty that data breaches create, many jurisdictions are looking to bring their data protection legislation in line with the new, internet-based world — although unfortunately, not into alignment with each other.

However, there is a fundamental transformation underway. In the digital economy, information is the currency of exchange and information knows no boundaries. Harmonization of regulations that fosters the free flow of information — while strengthening privacy and security rights — is an imperative for policy makers.

Take the EU and US trading block as an example. The total value of goods and services between the two largest trading blocks is estimated at $5.5 trillion, employing 15 million people. Cross border flows between the EU and the US are estimated to be 50% higher than any other trading block. 65% of US investment in information technology is in the EU. Harmonization of privacy regulations is needed to foster consumer confidence, harness information for sustainable competitive advantage and to strengthen corporate reputation as responsible stewards in the management of personally identifiable information.

There are a number of vexing challenges associated with the inevitable shift toward harmonization of privacy regulations. In the US, privacy is industry specific and enforcement is largely dependent on the sensitivity and commercial value of the information to be protected (e.g. Health Insurance Portability and Accountability Act, Fair and Accurate Credit Transaction Act). However, US regulatory agencies are now adding more teeth to privacy enforcement actions. This can be seen in the Federal Communications Commission levying a fine of $25 million against AT&T for the unauthorized disclosure of 280,000 customer records in 2015.

Historically the EU has had a high bar for privacy protection. Privacy is considered to be a fundamental human right and Article 7 of the EU Charter of Human Rights stipulates that "everyone has the right to respect…private and family life, home and communications." EU Privacy initiatives — including the EU Privacy Directive that preceded the European General Data Protection Regulation — are based on the preservation of privacy rights as an immutable principle.

The General Data Protection Regulation (GDPR) was a response to: 1) advances in digital technologies such as big data, cloud computing and predictive analytics; and 2) revelations of bulk data collection and profiling by intelligence services. The result is a comprehensive overhaul of privacy legislation and a considerable strengthening and expansion of privacy rights.

The scope of GDPR includes more rigorous consent requirements, data anonymization, the right to be forgotten and breach notification requirements. Violations could lead to fines of up to €20 million or 4% of global annual turnover for the preceding financial year — whichever is the greater — being levied by data watchdogs. For other breaches, the authorities could impose fines on companies of up to €10m or 2% of global annual turnover — whichever is greater. For the average Fortune 500 company, that puts fines in the range of $800-900M.

Today, data subjects face daunting challenges in providing informed consent to the data controllers and processors who are collecting their personal information. A report by the World Economic Forum found that, on average, data subjects have to invest 250 working hours, or 30 working days each year, just reading privacy notices in order to provide informed consent. Given the challenges associated with providing affirmative and informed consent, there is an emerging school of thought based on the use model which aims to shift away from the traditional notice and consent model to mandating that data controllers and processors guard against "harmful" uses of personally identifiable information. Implicit in the use model is increased accountability and transparency by data processors and controllers as well as more rigorous enforcement measures in the event of infringement.

Then there is a growing tension between protection of privacy rights and national security interests. Balancing privacy rights and national security interests is an on-going concern for policy makers. A 2016 survey by Pew Research Center found that while 56% of survey participants want more to be done to keep the country safe, 52% remain seriously concerned that the scope of surveillance programs may intrude upon their privacy, particularly when it comes to monitoring of internet search habits, email messages and social media interactions.

This tension between privacy and national security came to prominence when the Department of Justice sought for Apple to create a backdoor for the FBI to bypass iPhone encryption in order to access information that would potentially uncover activities of two terrorists who killed 14 people in San Bernardino. Apple, in their filing, put forth a passionate defense for preserving privacy rights on both technical and legal grounds. Apple's position was reinforced by the Electronic Frontier Foundation, arguing that "It would be great if we could make a backdoor that only the FBI could walk through. But that doesn't exist. And literally every single mathematician, cryptographer, and computer scientist who's looked at it has agreed."

The bottom line is that in the absence of harmonization, digital commerce may be adversely impacted. In many ways the EU is leading the way toward a fundamental overhaul of privacy protection that brings it in line with the realities of digital commerce. Resistance may be both futile and counterproductive to the promotion and growth of digital commerce.

Action Item: Universally accepted privacy principles, based the OECD Guidelines for the Protection of Privacy, include:

- *Specifying the purpose associated with the collection of personally identifiable information;*
- *Informed consent;*
- *Limiting use to the specific purposes to which data subjects consented;*
- *Transparency;*
- *Data quality; and*
- *Security, auditing and accountability.*

The OECD Guidelines have been codified in various Privacy legislations across the developed world, including in the US.

2 What is GDPR, why should you care, and what does it mean for your organization?

A new set of European rules and standards related to privacy and data protection (the General Data Protection Regulation, or GDPR) has set in motion a mad compliance and security scramble not only for European companies, but also for any company doing business in Europe or with European customers. The regulation is designed to harmonize privacy across the EU, codify more rigorous privacy rights and strike a balance between privacy and security and create an explicit obligation for both data controllers and processors to demonstrate compliance with GDPR. The clock is ticking – the regulation goes into effect on May 25th, 2018, and the potential penalties for non-compliance are significant (organizations found to be in breach of GDPR may be fined up to 4% of annual revenues or 20 million Euro, whichever is the greater).

This is not just a problem for European-based companies. If your organization does business in the EU, offers goods and services to EU citizens, or processes EU citizen data, then all the provisions of GDPR apply, including:

- More rigorous data security measures *to protect the confidentiality, integrity and availability of personal information, including provision for technical measures such as encryption. Data controllers and processors must limit collection to only the purposes for which consent was obtained.*
- A higher bar for obtaining consent, *which must be in the form of a clear affirmative action. This higher standard contrasts with the previous EU Directive, which allowed for implicit opt in consent. This higher bar extends to tracking cookies designed to identify a device and/or individuals across the web.*
- New breach notification provisions *with considerably more teeth, rendering fines that may potentially be as high as (or even exceed in the case of smaller companies) 4% of annual revenues. The definition of "data breach" is a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."*
- *The need to offer a choice by which data subjects may opt out of the disclosure or use of data, particularly when the intended disclosure or use is inconsistent with the original purpose for which the data was collected.*
- *The ability for the data subject to access, correct and delete any inaccurate information, including a "right to be forgotten."*
- New governance over data and data processes, *including specific appointments of a Chief Privacy Officer (CPO) and specific recommendations and provisions for Board of Director responsibilities to comply with the privacy regulation.*
- *Cross border transfer of EU citizen data must be subject to the adequacy standard. Furthermore, as a direct response to the Snowden revelations relating to the bulk collection of personal data, the European Commission and the US Department of Commerce have jointly developed a new framework for onward transfer under the EU-US Privacy Shield Framework, which supplants the previous Safe Harbor provisions.*

The new Privacy Shield considerably strengthens the privacy rights of EU citizens relating to onward transfer of personal information. Key provisions of the Privacy Shield require adherence to the core privacy principles of notice, choice, security, integrity, access, enforcement and accountability for onward transfer.

Perhaps the most important aspect of the Privacy Shield is more rigorous access, monitoring and enforcement mechanisms that were lacking in Safe Harbor. According to the European Commission's statement, "for the first time, the US has given the EU written assurance that the access of public authorities for law enforcement and national security will be subject to clear limitations, safeguards, and oversight mechanisms and has ruled out indiscriminate mass surveillance of European citizens' data." By virtue of these strengthened enforcement mechanisms, EU citizens will be able to:

- *Seek redress for alleged privacy rights against companies who are obliged to resolve such complaints within 45 days;*
- *Gain access to an Independent Dispute Resolution at no cost;*
- *Work through EU Data Protection Authorities, who are empowered to work with the US Federal Trade Commission (FTC) to ensure that EU citizen complaints are addressed and remedied;*
- *Opt for arbitration should their complaints not be resolved through the independent Dispute Resolution mechanism; and*
- Rely on Presidential Policy Directive No 28 (PDP 28), *which extends privacy protections to foreigners.*

It remains to be seen how recent developments within the EU and US will impact implementation of the new Privacy Shield. The European Parliament remains concerned about the efficacy of the Privacy Shield, and the current US Administration's resolution designed to roll back privacy protections relating to browser history collected and sold by internet service providers is a cause for concern among EU regulators. Recently, officials from the US Government and the EU Commission and Data Protection Authorities met in Washington to review the status of the Privacy Shield, which governs the transfer of EU data to US data controllers and processors. The results of the review are pending. This review is considered pivotal for the continued legal framework for trans-border data flows that constitute a significant dimension of commerce between these two large trading blocks.

In the meantime, the Irish High Court recently referred the high profile Schrems case to the Court of Justice of the EU, assessing the validity of standard contractual clauses for the transfer to EU personal data to jurisdictions outside the EU, in particular the US. Schrems is a landmark decision that invalidated the Safe Harbor provisions for trans-border data transfers given the bulk collection practices of US law enforcement agencies. The decision by the Irish High Court to refer the validity of standard contractual clauses further muddies the waters as to the conditions under which EU personal data may be transferred to data controllers and processors in the US.

3 What does "Privacy by Design" Mean?

Organizations must consider the concept of Privacy by Design moving forward, which attempts to embed privacy principles within privacy best practices, systems and software.

Formulated by the Privacy Commissioner for the Province Ontario, Privacy by Design encompasses seven foundational principles for embedding privacy within systems and software. Privacy by Design principles were espoused by International Conference of Privacy Commissioners "as a holistic concept that may be applied throughout the organization, including its technology and business practices."

GDPR has entrenched Privacy by Design, requiring data processors and controllers to "implement appropriate technical and organizational measures for ensuring that by default only personal data necessary for each specific purpose of the processing are processed."

One of the key foundational tenets of Privacy by Design is that privacy rights ought to be protected and enforced by *default* in order to proactively mitigate privacy risks. From a software and process design perspective it means that Privacy by Design should encompass:

- ***Data Minimization:*** *to restrict collection to the minimum amount of personally identifiable information required for processing;*
- ***Data Classification:*** *to ensure that personally identifiable information is tagged and assigned the appropriate level of protection from exposure;*
- ***Data Pseudonymization and Encryption:*** *to ensure the ongoing confidentiality, integrity, availability and resilience of personal data and data systems, and to preserve privacy through the processing of personal data in ways that can no longer be attributed to a specific data subject;*
- ***Data Aggregation:*** *to provide for tools to aggregate personally identifiable information to the highest level;*
- ***Auditing and Control:*** *to provide data subjects with agency over their personal information and which empowers data processors to demonstrate compliance; and*
- ***Intuitive User Interface Design:*** *to enable users to easily understand privacy notices, to provide affirmative consent (since under GDPR implied consent is no longer permissible) and to withdraw consent by providing intuitive access to privacy settings including simple to understand privacy icons.*

4 How will the Internet of Things (IoT) make the privacy equation even more complicated?

A recent Gartner report estimates that by 2020 the number of connected devices such as sensors and wearables will reach 21 billion, up from 6.4 billion in 2016. Such an unprecedented level of connectedness is expected to transform virtually every facet of our lives, largely in beneficial ways.

There are increasing concerns as to how pervasive use of IoT devices will impact privacy rights. It's not just the volume of data generated, but also the variety of information collected, such as geolocation, internet search habits and preferences which, taken together, may infringe upon privacy rights. A recent Ponemon report found that while there is no real standard governing IoT privacy, there is a preference for some form of "labeling" associated with IoT devices that communicate in plain language the information they collect.

Is obtaining informed consent practical when it comes to the world of IoT? There is an emerging school of thought that holds that the traditional consent model ought to be supplanted by a use model given that "ensuring individual control over personal data is not only an increasingly unattainable objective of data protection, but in many settings it is an undesirable one, as well." The rationale for this proposed overhaul of traditional notions of privacy is that "there are compelling societal benefits to the collection and use of personal information as long as it is anonymized and aggregated so as to preclude identification of the data subject."

This includes de-identification of personally identifiable information and adherence to higher accountability standards, including payment of fines in the event of infringement causing harm. The use model acknowledges the impracticality of obtaining informed consent. Rather, it places emphasis on the benefits associated with de-identified personal data that delivers social utility, such as health-care prevention, more efficient transportation, environmental protection and education. While privacy in the age of the IoT is nascent, the legal framework based on informed consent has been considerably strengthened with the ratification of GDPR. The onus is clearly on organizations to implement and adhere to rigorous information governance best practices that empower them to capture, classify and use personally identifiable information in accordance with privacy regimes based on informed consent.

There are a number of new initiatives that show promise in balancing privacy rights and social utility. For example, the 2013 World Economic Forum report proposes that personal data be tagged, and includes terms under which such data may be used, including an audit function that verifies compliance. There is a potentially useful technical initiative — "eXtensible Access Control Markup Language" (XACML) — designed to embed privacy settings by tagging data with privacy preferences. The Federal Trade Commission Staff Report recommends the use of QR codes that provide details as to information collected by IoT devices and a provision for privacy choices during device installation. Finally the Online Trust Alliance, a consortium of IoT device manufacturers, proposes rigorous disclosure policies prior to purchase, including ability to control privacy settings.

5 What should your organization do about all of this, and what role will machine learning play in solving the privacy problem?

Your organizational strategy needs to start with a commitment to sound information governance policies and practices. Having in place a well-defined and clearly articulated set of information governance best practices empowers organizations to not only mitigate risk, but also to leverage information assets for competitive advantage.

Many organizations stop there, and make the mistake of assuming the old approaches based on a paper paradigm will be sufficient. Information management and privacy challenges created by an explosion in the volume of information cannot be solved by the old manual approaches. Machine learning technologies — such as intelligent capture and classification to digitize incoming information, identify patterns in data collected, and organize, preserve and protect data — must be a key part of the solution.

Technologies such as document capture, pattern recognition and knowledge management are widely used to automate the digitization of documents without human intervention and with a high degree of accuracy. And finally, organizations need to better align data and document security policies with information governance. These regulations require more flexible and persistent privacy protections throughout the information management lifecycle that must be built into the systems themselves.

With the advent of big data and cloud computing, machine learning is pushing toward the next stage — deep learning. Deep learning is an advanced form of machine learning technology, the objective of which is to simulate the human mind. Current applications of deep learning such as fraud detection engines and predictive analytics are the first wave of the technology, and empower organizations to gain granular insight into consumer sentiments and behavior, and make decisions without human intervention.

While deep machine learning creates compelling commercial benefits, it also elicits a new set of privacy concerns. The U.S. supreme Court decision in Riley has recognized the potentially adverse consequences of profiling based on the collection of metadata. GDPR anticipates the inherent challenges associated with deep learning technologies, and empowers data subjects with a right to object profiling based on automated processing of metadata collected from browsing history.

The EU ePrivacy legislation, which was amended and incorporated into GDPR, requires affirmative consent to place tracking cookies on consumer's internet browsers. These amendments prohibit opt in consent to collect personal information by tracking cookies, including pre ticked boxes. Applications must provide settings that enable users to:

- *Prevent the storing of information by third parties for tracking purposes;*
- *Control the degree to which tracking cookies may be stored; and*
- *Provide such options in clear, concise and transparent manner.*

There are proven instances of machine learning that can help organizations with GDPR compliance. Intelligent Document Capture (IDR) uses advanced document recognition and classification algorithms.

With this technology, incoming documents are analyzed based on their content and metadata, and then automatically classified without human intervention. Through such document understanding, personally identifiable information embedded in documents may be identified, tagged, classified and assigned the requisite level of privacy settings and protection.

Concept Searching (Semantic Analysis) is an advanced machine learning technology that finds and relates documents based on their content and the subject matter of the document, paragraph, or sentence. Concept searching enables organizations to "discover" their information holdings across multiple disparate repositories, such as email, file shares, and social media, then identify documents that may contain personally identifiable information and apply appropriate rules to govern their collection, use and disposition.

The bottom line: compliance with GDPR is a strategic imperative to effectively compete in digital economy.

Some Suggested Resources:

A useful starting point to consider is the Information Governance Reference Model (IGRM). The IGRM model is an extension of ARMA's Generally Accepted Recordkeeping Principles.

The Information Governance Reference Model is based on three key pillars:

- *Managing information as a strategic competitive asset:*
- *Accessibility of information to ensure IT efficiency; and*
- *Compliance with legal and regulatory frameworks, including records retention, disposition, data privacy and security.*

In order to ensure adherence to these information governance principles, organizations ought to apply end-to-end information life cycle processes that encompass:

- *Information capture and classification;*
- *Protection of personally identifiable information;*
- *Control of the collection and use of personally identifiable information;*
- *Detection of data breaches;*
- *Response to and mitigation of infringement of privacy rights; and*
- *Reporting and analytics to measure compliance with privacy regimes.*

There are a number of tools and best practices around privacy-related information. A particularly comprehensive resource is Nymity. This resource provides a wealth of information about GDPR compliance and accountability. GDPR mandates that organizations undertake privacy impact assessments, particularly when sensitive personal information is processed, when data subjects are profiled and new technologies are implemented that impact privacy rights. Having processes in place to conduct, benchmark, implement and measure the efficacy of privacy programs is imperative to ensure compliance

There are a number of useful resources that offer GDPR readiness and assessment tools. Microsoft offers a free resource kit that provides an intuitive guide consisting of 26 questions to gauge GDPR readiness. In addition, IAPP offers a comprehensive report of vendors that provides in-depth analysis of various tools to help organizations conduct due diligence in selecting their GDPR readiness solutions.

Is your organization ready to embrace a more rigorous privacy regime as espoused by GDPR? What is your organizational readiness to comply with GDPR when it becomes effective in May 2018? A recent survey by PwC shows that companies are planning to spend between $1 million and $10 million to comply with GDPR. How do you stack up?

AIIM provides useful resources to help your organization gain insight to these important considerations relating to GDPR, and a number of sponsor resources are listed in the sponsor section of this e-book.

About FileFacets

FileFacets is an online privacy compliance and enterprise analytics platform that makes it easy for businesses to locate and action content from multiple sources across the entire organization to help protect sensitive data and mitigate risk. The platform performs sophisticated data discovery and content search of structured and unstructured content within corporate networks, servers, enterprise content management systems (ECMs), email, desktops and laptops.

GDPR Planning for Data Protection - The first step in understanding what personal data an organization holds is to understand exactly ***how much data*** they have, where it is, and what it is. FileFacets gives businesses a unified view of all their content across the entire organization, arming them with the tools and the methodology to help them comply with the data protection and information management requirements of the European Union's General Data Protection Regulation (GDPR) – from planning through to execution of a business' GDPR strategy.

Data Subject Access Rights - FileFacets can easily locate, identify, audit and action files containing the personal data of an individual regardless of its location within an organization's data stores, including emails and desktops. This capability allows businesses to meet the requirements of Chapter 3's Subject Access Requests (SAR) articles including the ***Right to Access and Portability:*** where an individual requests to view and retain a copy of all of their personal data, and the ***Right to be Forgotten:*** where an individual requests to have their personal data removed from a business' data stores.

Reporting for Transparency & Accountability - FileFacets audit and reporting capabilities allows for transparency and accountability for internal governance: by auditing users' decisions on the requests and actions of files and file types; for an individual's ***Right to Notification:*** with the ability to report on compromised data in the case of a breach of their personal data; and to external Data Protection Authorities (DPA) by identifying all documents and records containing personal data that may have been affected in the event of a data breach.

For more information on how FileFacets can help your organization with GDPR planning, readiness and compliance, download our whitepaper:
FileFacets for GDPR – Solution Overview for Compliance.

FileFacets
20 Cope Drive,
Ottawa, ON K2M 2V8,
Phone: 1.877.213.743,
Email: contact@filefacets.com
Web: www.filefacets.com

You've just downloaded and read the latest AIIM Intelligent Information eBook on GDPR.

What now?

Take your skills to the next level by learning how to map, design, capture and automate operational processes using a combination of strategies, and technologies with AIIM's Training Courses

Learn more, visit: www.aiim.org/training

AIIM
1100 Wayne Avenue, Suite 1100
Silver Spring, MD 20910
(+1) 301 587-8202
www.aiim.org

AIIM Europe
Office 1, Broomhall Business Centre
Broomhall Lane, Worcester, WR5 2NT, UK
+44 (0)1905 727600
www.aiim.org